State of Arizona

Department of Economic Security Information Technology Standards	Title: 1-38-0075 DES Physical Security Policy	
Subject: This policy defines required physical and environmental security controls for DES.	***Effective Date:*** 03/07/05	***Revision:*** 1

1. Summary of Policy Changes

1.1. Original Implementation

2. Purpose

The purpose of this policy is to prevent unauthorized access, damage, and interference to business premises and information belonging to the Arizona Department of Economic Security.

3. Scope

3.1. This policy applies to all DES administrative entities, councils, divisions, administrations, programs and non-DES entities that affect DES facilities and/or systems.

4. Responsibilities

4.1. The DES Director, Deputy Directors, Associate Director, and Assistant Directors are responsible for implementing and enforcing this policy.

4.2. The DES CIO and the DES Division of Technology Services is responsible for implementing this policy.

4.3. DES divisions and programs are responsible for implementing this policy and monitoring compliance.

5. Definitions and Abbreviations

5.1. Abbreviations

5.1.1. **AHCCCS** – **A**rizona **H**ealth **C**are **C**ost **C**ontainment **S**ystem

5.1.2. **CIO** – **C**hief **I**nformation **O**fficer

5.1.3. **CISO – C**hief **I**nformation **S**ecurity **O**fficer

5.1.4. **DTS** – **D**ivision of **T**echnology **S**ervices

5.1.5. **DES** – **D**epartment of **E**conomic **S**ecurity

5.1.6. **GITA** – **G**overnment **I**nformation **T**echnology **A**gency

5.1.7. **IT** – **I**nformation **T**echnology

5.1.8. **ISA** – **I**nformation **S**ecurity **A**dministration

6. Policy

6.1. Secure Areas

Objective*:* To prevent unauthorized access, damage, and interference to business premises and information.

Critical or sensitive business information processing facilities will be housed in secure areas, protected by defined security perimeter, with appropriate security barriers and entry controls. They will be physically protected from unauthorized access, damage, and interference.

6.2. Physical entry controls

Secure areas are defined as areas that contain sensitive information assets or sensitive

information processing facilities.
Secure areas will be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. The following guidelines must be followed in the case of secure areas:

a) Visitors to secure areas will be supervised or cleared and their date and time of entry and departure recorded. They will only be granted access for specific, authorized purposes and will be given instructions on the security requirements of the area and on emergency procedures.
b) Access to sensitive information and information processing facilities will be controlled and restricted to authorized persons only. Authentication controls, e.g. swipe card, will be used to authorize and validate access. An audit trail of all access will be securely maintained.
c) All personnel will be required to wear some form of visible identification (e.g. a DES issued badge with photo) and will be encouraged to challenge unescorted strangers and anyone not wearing visible identification.
d) Access rights to secure areas will be regularly reviewed and updated as part of the Information Security Risk Assessment Program. (See Security Risk Assessment Procedure for details.)

6.3. Securing offices, rooms, and facilities

A secure area may be a locked office or several rooms inside a physical security perimeter, which may be locked and may contain lockable cabinets or safes. The selection and design of a secure area will take account of the possibility of damage from fire, flood, explosion, civil unrest, and other forms of natural or man-made disaster. Account will be taken of relevant health and safety regulations and standards. Consideration will be given also to any security threats presented by neighboring premises, e.g. leakage of water from other areas.
Furthermore:

a) Key facilities will be located to avoid access to the public.
b) Buildings will be unobtrusive and give minimum indications of their purpose, with no obvious signs outside or inside the building identifying the presence of information processing facilities.
c) Doors and windows will be locked when unattended and external protection will be considered for windows, particularly at ground level.
j) All card access to secured areas will be monitored by qualified security personnel and any unusual incidents will be investigated per the guidelines of the Incident Response policy.

6.4. Equipment security

Objective: *To prevent loss, damage, or compromise of assets and interruption to business activities.*

Equipment will be physically protected from security threats and environmental hazards. Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. This will also be considered for equipment location and disposal. Special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting facilities, such as electrical supply and cabling infrastructure.

6.4.1. Equipment location and protection

Equipment will be located or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

a) Equipment will be located to minimize unnecessary access into work areas.
b) Information processing and storage systems handling sensitive data will be positioned to reduce the risk of overlooking during use.
c) Items requiring special protection will be isolated to reduce the general level of protection required.
d) Controls will be adopted to minimize the risk of potential threats to include:
theft; sabotage; fire; explosives; smoke; water; dust; vibration; chemical effects; electrical supply interference; electromagnet radiation.
e) DES will limit areas in which eating, drinking, and smoking in proximity to information processing systems is conducted (e.g. the Data Center). Signs declaring: "No food or drink allowed in the areas" will be prominently posted throughout the area.
f) Environmental conditions will be monitored for conditions which could adversely affect the operation of information processing facilities.
g) The impact of a disaster happening in a nearby premises, e.g. a fire in a neighboring building, water leaking from the roof or in floors below ground level or an explosion in a street must be considered.

6.5. Power Supplies

Equipment will be protected from power failures and other electrical anomalies. A suitable electrical supply will be provided that conforms to the equipment manufacturer's specifications.

Options to achieve continuity of power supplies include:

a) Multiple feeds to avoid a single point of failure in the power supply;
b) Uninterruptible power supply (UPS);
c) Back-up generator.

A UPS to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Contingency plans will cover the action to be taken on failure of the UPS. UPS equipment will be regularly checked to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations.

A back-up generator will be considered if processing is to continue in case of a prolonged power failure. Generators will be regularly tested in accordance with the manufacturer's instructions. An adequate supply of fuel will be available to ensure that the generator can perform for a prolonged period.

In addition, emergency power switches will be located near emergency exits in equipment room to facilitate rapid power down in case of an emergency. Emergency lighting will be provided in case of main power failure. Lightning protection will be applied to all buildings and lightning protection filters will be fitted to all external communications lines.

6.6. Equipment maintenance

Equipment will be correctly maintained to ensure its continued availability and integrity, with the following guidelines:

a) Equipment will be maintained in accordance with the supplier's recommended service intervals and specifications.
b) Only authorized maintenance personnel will carry out repairs and service equipment.
c) Records will be kept of all suspected or actual faults and all preventative and corrective maintenance.
d) Appropriate controls will be taken when sending equipment off premises for maintenance.
e) All requirements imposed by insurance policies will be complied with.

6.7. Storage of backup media

All media that is part of the data backup process must be stored either in a fireproof safe onsite or offsite with an appropriate third party vendor. A data retention scheme that complies with applicable Department legal and operational requirements will be followed. Refer to the Data Retention Policy for more information.

6.8. General Controls

Objective: *To prevent compromise or theft of information and information processing facilities.*

Information and information processing facilities will be protected from disclosure to, and modification of or theft by unauthorized persons, and controls will be in place to minimize loss or damage.

6.9. Clear desk and clear screen policy

The Department has a clear desk guideline for confidential papers and removable storage media and a clear screen guideline for information processing systems in order to reduce the risk of unauthorized access, loss of, and damage to information during and outside normal working hours. The guidelines will take into account the information security classifications, the corresponding risks and cultural aspects of the Department.

Information left out on desks is likely to be damaged or destroyed in a disaster such as a fire, flood, or explosion. The following guidelines must be followed:

a) Where appropriate, paper and computer media will be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours.
b) Confidential business information will be locked away (ideally in a fire resistant safe or cabinet) when not required, especially when the office is vacated.
c) Computers, computer terminals and printers will not be left logged on when unattended and will be protected by key locks, passwords, or other controls when not in use. These controls include a password protected screen saver. Please reference Session Standard policy for details.
d) Incoming and outgoing mail points, as well as unattended fax machines will be protected.
e) Photocopiers will be locked (or protected from unauthorized use in some other way) outside normal working hours.

f) Confidential information, when printed, will be cleared from printers immediately.

6.10. Personnel Security

General emergency procedures (e.g. fire, bomb threat, other emergencies) will be in place for each facility of the Department. These procedures will be tested twice annually and maintained on a regular basis by Facilities Management.

7. Implications

DES business units must review their existing rules and processes and change them to suit this policy.

8. Implementation Strategy

This policy is effective for all DES business units as of its publication.

9. References

9.10. None

10. Attachments

10.10. None

11. Associated GITA IT Standards or Policies

11.10. None

12. Review Date

12.1. This document will be reviewed twelve (12) months from the original adoption date, and every twelve months thereafter.